KIST 한국과학기술연구원

행정·연구지원부문(IT 인프라(서버/정보보안) 분야) 직무기술서

채용분야	IT 인프라(서버/정보보안)				
대분류	20. 정보통신				
중분류	01. 정보기술				
소분류	02. 정보기술개발		03. 정보기술운영	06. 정보보호	
세분류	02. 응용SW엔지니어링	06. 보안엔지니어링	01. IT시스템관리	01. 정보보호관리·운영	03. 보안사고분석대응
주요사업	미래 선도 원천기술 확보, 국가·사회적 현안 해결기술 개발, 융합·협력 개방형 플랫폼 구축				
능력단위	○ **(응용SW엔지니어링)** 01. 요구사항 확인, 05. 데이터 입출력 구현, 06. 통합 구현, 08. 정보시스템 이행, 11. 서버 프로그램 구현, 12. 인터페이스 구현, 18. 인터페이스 설계 ○ **(보안엔지니어링)** 01. 보안 구축 계획 수립, 03. 보안 구축 요구사항 분석, 04. 관리적 보안 구축, 10. 보안인증 관리, 12. DB보안 구축, 13. 시스템 보안 구축 ○ **(IT시스템관리)** 01. IT시스템 운영 기획, 03. IT시스템 서비스 수준관리, 08. DB 운영관리, 09. 보안 운영관리, 11. IT시스템 통합운영관리, 12. IT시스템 통합운영안정성관리, 15. IT시스템 서버 운영관리, 19. IT시스템 변경관리 ○ **(정보보호관리·운영)** 05. 보안 위험관리, 06. 정보보호 계획 수립, 08. 네트워크 보안 운영, 10. 시스템 보안 운영, 14. 보안성 검토 ○ **(보안사고분석대응)** 03. 디지털 포렌식, 04. 사이버조사, 05. 침해사고 분석, 06. 악성코드 분석, 07. 보안로그 분석, 08. 보안사고 대응				
직무수행 내용	○ **(응용SW엔지니어링)** 컴퓨터 프로그래밍 언어로 각 업무에 맞는 소프트웨어의 기능에 관한 설계, 구현 및 테스트를 수행하고, 사용자에게 배포하며, 버전관리를 통해 소프트웨어의 성능을 향상시키고, 서비스를 개선하는 업무 ○ **(보안엔지니어링)** 정보보호 및 개인정보보호 관련 법률/정책 등의 이해를 바탕으로 연구원 정보보호정책을 수립하고 네트워크/시스템에 적용/운용하는 업무 ○ **(IT시스템관리)** 정보시스템을 안정적이고 효율적으로 운영하고 관리하기 위하여 하드웨어 및 소프트웨어의 지속적 점검과 모니터링을 통해 제시된 제반 문제점들을 분석하여 사전 예방활동 및 발생된문제에 대해 적절한 조치를 수행하는 업무 ○ **(정보보호관리·운영)** 연구원의 비전과 미션을 수행하기 위하여 정보 자산을 안정적으로 운영하는 데 필요한 정보보호 전략 및 정책을 수립하고, 관련 법제도 준수, 정보보호관리 활동을 수행하며, 위험관리에 기반한 정보보호 대책을 도출하고 실행하는 업무 ○ **(보안사고분석대응)** 연구원 사이버공격 및 침해사고의 예방활동, 위협정보를 탐지/분석, 피해 현황 파악 및 복구 등 침해사고 대응절차를 수행하는 업무				
필요지식	○ **(응용SW엔지니어링)** 요구사항 분석 기법, SQL(Structure Query Language), 시스템 성능 분석 및 진단 방법, 소프트웨어 개발 프레임워크, 객체지향 프로그래밍 언어, E-R(Enitity-Relationship) 모델링 기법 ○ **(보안엔지니어링)** 정보보호관리체계에 관한 국제표준 규격(ISO27001), 정보보호 및 개인정보보호 관리체계(ISMS-P), 서비스 공격유형, 시스템 아키텍처, 암호알고리즘, 접근통제, 식별 및 인증, 보안 솔루션 종류 및 유형별 제공 기능, 네트워크 기반 공격유형 및 QoS, 소프트웨어 개발 보안 가이드, 프로그래밍 언어 ○ **(IT시스템관리)** 서버/네트워크/소프트웨어 관리 방법, 위험관리 방법, 서버/스토리지/네트워크/소프트웨어 관련 운영 기법, 데이터베이스 관리시스템, 데이터베이스 테이블 설계 기법 ○ **(정보보호관리·운영)** 정보보호시스템 운영 정책, 정보시스템 보안 진단 및 취약점 진단/분석과조치, 물리적/관리적 보안운영 정책/이행 관련 지식 ○ **(보안사고분석대응)** 침입대응, 분석 실무에 필요한 정보수집 및 활용 방법, 침해사고 대응절차, 원인과 사고과정 분석에 관한 지식, 보안위협 이벤트/원리이론분석, 침해사고 관련 휘발성, 비휘발성 증거수집 방법, 네트워크와 시스템 취약점 관련 지식				

필요기술	○ **(응용SW엔지니어링)** 요구사항 검증 능력, SQL 활용 능력, APM(Application Performance Monitoring) 활용 능력, IDE(Integrated Development Environment) 도구 활용 능력, 프로그래밍 언어 및 도구 활용 능력, E-R 모델링 능력 ○ **(보안엔지니어링)** 시스템/네트워크 취약점분석 도구 사용기술, 로그분석 도구 사용 기술, 서버보안 소프트웨어 설치 및 운영기술, 보안 아키텍처 수립기술, 운영체제의 환경 설정 기술, 응용 프로그램 실행 제어 기술 ○ **(IT시스템관리)** 시스템 환경 구성 기술, 자원관리 기술, 네트워크 관리 기술, 서버/네트워크/소프트웨어 보안패치 및 업그레이드 기술, 데이터베이스 테이블 설계 기술 ○ **(정보보호관리·운영)** 정보보호 관련 법 및 규정 분석 능력, 정책/표준/지침/절차의 분석 능력, 정보보호 정책 체계 파악 능력, 정보자산의 구성과 현황 파악 기술 ○ **(보안사고분석대응)** 침해사고 분석 시술(분석도구, 원인, 사고과정 분석 등), 네트워크시스템 로그/보안취약점/분석 도구 사용기술, 악성코드 행위분석 기술, 파일/프로세스/레지스트리구조 동작방식
직무수행 태도	○ 고객의 요청에 대한 적극적인 수용, 다양한 가능성에 대해 유연하게 사고하는 태도, 이해관계자 의견을 경청하는 자세, 자신의 업무에 책임감을 갖고 역할을 다하려는 의지, 합리적인 사고능력을 기반으로 정확한 업무 수행을 위해 집중하려는 의지
자격사항	-
직업기초 능력	○ 의사소통능력, 수리능력, 자원관리능력, 문제해결능력, 조직이해능력, 외국어능력
참고	○ 위 직무기술서는 한국산업인력공단의 표준 분류를 참고하여 KIST에서 자체 작성한 직무기술서로, 향후 NCS 개발 동향 등 내·외부 사정에 따라 변경될 수 있음을 알려드립니다. ○ 참고사이트 : www.ncs.go.kr